AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

1. (**Currently Amended**) A method for protecting the transfer of data between a computer and [[a]] an external device, the method comprising the steps of:

a. receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device, said external device connected to the computer and communicating therewith via a physical communication port~~, the data portion being associated with a particular physical communication port of the computer and with the device that is currently communicating via the particular physical communication port~~;

b. ~~processing~~ analyzing, by said module, the data portion according to a protocol ~~that is~~ associated with the physical communication port;

c. determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if [[not]] no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a [[the]] next data portion, and if said decision may be reached [[yes]], then proceeding ~~proceed~~ to step 'd';

d. determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed, then [[yes]] transferring the one or more data portions with data ~~that are~~ stored in the associated buffer, if any exist, toward or from the physical communication port, and if [[not]] said data communication session is not

to be allowed, then modifying [[the]] data transportation related to said data communication session.

2. (**Currently Amended**) The method of claim 1, wherein the step of modifying the data transportation ~~further~~ comprises blocking the transportation.

3. (**Currently Amended**) The method of claim 1, wherein the step of modifying the data transportation ~~further~~ comprises modifying the type of the transportation.

4. (**Currently Amended**) The method of claim 1, wherein the step of modifying the data transportation ~~further~~ comprises modifying ~~the~~ a status of a requested file.

5. (**Currently Amended**) The method of claim 1, wherein the step of modifying the data transportation ~~further~~ comprises correcting the data according to the communication protocol.

6. (Original) The method of claim 1, wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

7. (Original) The method of claim 1, wherein the physical communication port is a USB port.

8. (Original) The method of claim 1, wherein the physical communication port is wireless.

9. (**Currently Amended**) The method of claim 1, wherein the step of ~~processing~~ analyzing the data portion further comprising:

(i) determining whether additional processing based on a higher level protocol is required, [[and]] wherein if additional processing is not

required, then continuing at step 'c', otherwise ~~continue~~ continuing at step (ii); and

(ii) processing part of the data portion ~~that is~~ relevant to the higher level protocol according to the higher level protocol and returning to step (i).

10. (**Currently Amended**) The method of claim 9, wherein the step of ~~processing~~ analyzing ~~part of~~ the data portion ~~further~~ comprises ~~processing~~ analyzing relevant to a higher level protocol that is associated with the external device.

11. (**Currently Amended**) The method of claim 10, wherein the data communication session ~~device~~ is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

12. (**Currently Amended**) The method of claim 1, wherein the step of ~~processing~~ analyzing the data portion is performed in respect of the data ~~that is~~ stored in the associated buffer.

13. (**Currently Amended**) The method of claim 1, wherein the step of determining whether a decision on the data communication session may be reached[[,]] is performed in respect of the data ~~that is~~ stored in the associated buffer.

14. (**Currently Amended**) The method of claim 1, wherein the step of determining whether ~~a decision~~ to allow the data communication session is performed in respect of the data ~~that is~~ stored in the associated buffer.

15. (**Currently Amended**) The method of claim 1, wherein the step of receiving a data portion ~~further~~ comprises receiving a data portion ~~that is~~ selected from a group consisting of packet and SCSI block.

16. (**Currently Amended**) The method of claim 1, wherein the step of receiving the data portion ~~further~~ comprises obtaining the data portion by emulating a class driver.

17. (**Currently Amended**) The method of claim 1, wherein step of receiving the data portion ~~further~~ comprises obtaining the data portion by emulating a filter module.

18. (**Currently Amended**) The method of claim 1, wherein the step of ~~processing~~ analyzing the data portion according to a protocol ~~that is~~ associated with the physical communication port further comprises:

i. parsing the data portion;

ii. reassembling the data; and

iii. analyzing the reassembled data.

19. (**Currently Amended**) The method of claim 1, wherein the step of determining whether to allow the communication session ~~further~~ comprises reviewing [[the]] a security policy.

20. (**Currently Amended**) The method of claim 1, wherein the step of determining whether to allow the communication session ~~further~~ comprises examining the working environment in which the computer is operating and [[only]] allowing the communication only if said computer is operating in one or more of [[for]] certain working environments.

21. (**Currently Amended**) A system for enhancing the security of a private network being accessed by a computer, the system comprising:

a client agent installed on a computer ~~that is communicatively coupled to the private network and is associated with a computer operating on the private network~~, the client agent having an associated security policy;

a security manager ~~that is~~ communicatively coupled to the private network;

wherein the client agent is ~~being~~ operative to:

detect a data transfer ~~passing~~ between [[a]] a hardware device connected to the computer through a physical communication port of the computer;

analyze the data transfer according to ~~the~~ a communication protocol associated with the physical communication port; and

verify whether the data transfer is allowable based on the analysis of the data and the security policy; and

wherein the security manager is ~~being~~ operable to associate a security policy with the client agent.

22. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy is correct.

23. (Original) The system of claim 21, wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session.

24. (Original) The system of claim 21, wherein the security policy includes a plurality of rules that at least define the type of operations that can be performed during a communication session.

25. (Previously presented) The system of claim 21, wherein the security manager is operable to disable any communication with the computer unless the client agent associated with the computer is active.

26. (**Currently Amended**) The system of claim 21, wherein the physical communication ports ~~can be~~ is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

27. (Previously presented) The system of claim 21, wherein the physical communication ports is a USB port.

28. (**Currently Amended**) The system of claim 21, wherein the physical communication [[ports]] port is wireless.

29. (Original) The system of claim 21, wherein the client agent is associated with the security policy by loading the security policy into the client agent.

30. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified.

31. (**Currently Amended**) The system of claim 21, wherein the client agent is further operative to transmit a report to ~~the~~ a security server, the report identifying events that occurred with the computer in view of the security policy.

32. (**Currently Amended**) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with [[a]] the hardware device, wherein the hardware device is selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.

33. (Original) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

34. (**Currently Amended**) A computer having installed thereon a module ~~software agent installed in a computer for enhancing the security of the computer, the agent being~~ operative to:

detect a data transfer passing through at least one physical communication port of the computer;

analyze the data transfer according to ~~the~~ a communication protocol associated with the at least one physical communication port; and

verify the data transfer is allowable based on the analysis of the data and a security policy.

35. (Previously presented) The method of claim 10, wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.

36. (**New**) The method of claim 1, wherein determining whether a decision on whether to allow the data communication session may be reached is based on a plurality of data portions, wherein at least one of said plurality of data portions is stored in said buffer.

37. (**New**) The method of claim 1, wherein determining whether to allow the data communication session is based on a plurality of data portions wherein at least one of said plurality of data portions is stored in said buffer.